



# Hacking y Pentesting con Python

Módulo 3: Hacking en entornos web con  
Python.

# Hacking en entornos web con Python

## ACTIVIDAD MODULO 3

### Objetivos

- | Preparar un entorno de pruebas para poder realizar prácticas de Hacking web con Python.
- | Aprender sobre las vulnerabilidades más comunes en aplicaciones y servidores web.
- | Utilizar las librerías más extendidas a la hora de crear clientes HTTP en Python.

### Contenido correspondiente a modulo 3:

1. Crear un entorno para realizar las pruebas en aplicaciones web vulnerables.
2. Utilizar Python para ejecutar ataques de forma automatizada contra aplicaciones web vulnerables.

### Actividad relacionada con el módulo 3:

Es necesario instalar la aplicación web vulnerable DVWA, para ello se recomienda utilizar Docker tal como se explica en el siguiente post: <https://thehackerway.com/2021/09/20/preparacion-de-un-entorno-con-docker-para-hacking-web/>

Crear un script que utilizando las librerías habituales para pentesting web descritas en la formación ejecute las siguientes actividades:

- Realizar de forma automática el proceso de autenticación en la aplicación web vulnerable DVWA.
- Una vez autenticado, cambiar el nivel de seguridad web a “Bajo”.
- Explotar la vulnerabilidad de OS Commanding de forma automática.
- Explotar una de las vulnerabilidades de SQL Injection disponibles en la aplicación.